5.0 Appendix A: Business Rules

5.0 Appendix A. Business Rules

Business Rules are used by WASS to assign privileges are described in a series of Tables that relate to the several functions. Table 5-1 describes a sampling of the rules for managing relationships with Business Partners.

Table 5-1 Maintain Business Partner Business Partner Business Rules/Functional Requirements

Requirement Description
A BPR Coordinator cannot activate or terminate user IDs of a BPR organization. Only Original Coordinators can activate or terminate user IDs from his organization
An Original Coordinator may deactivate a BPR Coordinator, but a BPR Coordinator cannot deactivate an Original Coordinator
A Super Administrator and System Administrator can activate a BPR Coordinator without entering an activation key code
An individual must first be an Original Coordinator in order to initiate a request to be granted BPR Coordinator status
The CEO of an organization must approve the request for a BPR before a BPR Coordinator can be activated
A Tax ID/SSN/PHA ID must be a valid HUD trusted business partner to be accepted for a business partner relationship
Only a Super Administrator or System Administrator can activate a deactivated BPR
An Original Coordinator can activate a requested BPR Coordinator
A Super Administrator or System Administrator can activate a BPR without entering the activation key code
An Original Coordinator or BPR Coordinator must enter the activation key code to activate a BPR
Only a System Administrator or Super Administrator can deactivate a requested BPR

Table 5-2 provides some of the Business Rules that describe assignment of roles and actions.

Table 5-2 WASS Business Rules/Functional Requirements

Requirement Description
ASSIGNMENT
Coordinator/System Administrator must do User Maintenance - Role Assignment function on User before a PHA Assignment can be completed for User.
Coordinator/System Administrator must do User Maintenance - Role Assignment function on User before an Assistance Contract Assignment can be completed for User.
Coordinator/System Administrator must do User Maintenance - Role Assignment function on User before a Property Assignment can be completed for User.
Coordinator can only assign to User property that Coordinator represents
Coordinator can only assign to User PHA that Coordinator represents
Users can only be assigned to property that is owned by the individual or organization under which they are registered (identified by TIN/SSN)
Selection of property to assign may be based upon property ID, FHA number, or Contract number.
Limit of 150 PHAs can be assigned to external Users. There is no limit to number of PHAs that can be assigned to internal Users.
In order for a Coordinator to assign Users to contract(s) the participant(s) the Coordinator represents must own property that have contracts on contract participant table.
System Administrators must select either a PHA ID or State for assigning PHA to User. Coordinators have the option of leaving the PHA ID and State fields blank in PHA Assignment.
User ID being assigned to property, PHA, contract, or participant must be active.
A maximum of 250 participants can be assigned to a User.

Systems Administrators and Super Administrators are the only ones that assign systems. The System Administrator can only assign USERS to his subsystem. It is a function that used to exist on a prior version of WASS. In WASS 3.0.0.0 it is a limited function. Most of the required system assignment is done through the registration process. This precludes assignment of systems that do not relate to the responsibilities of a Coordinator or a Regular USER.

Table 5-3 Maintain System Business Rules

Requirements Description
An individual must to be a Super Administrator (SA) in order to perform System Maintenance
A system cannot be deleted until all roles that are associated with the system are deleted
In order to do a System Delete an SA must also be the administrator for that system
A role cannot be deleted if it is used by another system
Group Maintenance is the only System Maintenance function that Coordinators can perform

User accounts are monitored. Table 5-4 provides the reasons for terminating an account and reasons for reactivating an account.

Table 5-4 Reasons for Terminating and Reactivating a User Account

Description for Terminating a User Account	Reasons for Reactivating a User Account
Resigned from employer	Unlocked account
Terminated by employer	Hired by employer
Locked by WASS because of inactivity	Re-hired by the employee
Locked by WASS because of excessive failed login attempts	Changed positions at the employer
Changed positions at the employer	Some other reason that is listed above

Table 5-5 describes the business rules for processing a request for access to subsystems. Satisfaction of the conditions described will provide access.

Table 5-5 Business Rules for Processing User Authentication

Description
Users must provide a valid Active User Id and password combination to login to WASS system.
Internal User's User Id/Password combination is checked for existence on the user information table.
External User's User Id/Password combination is checked for existence on the Lightweight Directory Access Protocol (LDAP). The LDAP is a database with all the User ID and passwords. The user information table is only checked for the existence of the User Id.
Internal and External Users must exist in the user information database and have an active status. External Users must also exist on the LDAP.
If WASS login fails, increment the counter for that user.
If the number of failed login attempts exceeds the limit, then lock the account and notify the user. Otherwise, you will be notified that the user ID and password are invalid.
If WASS login is successful, display WASS Main Menu to the User.
If User is External, display popup message about browsers then Display legal warning screen before displaying WASS Main Menu.
If User's password is 'password' OR User's password is expired (unchanged for 21 days) then, prompt user to change password before logging into WASS.
If User is an Inspector AND an USDA User, then display PASS USDA Menu instead of WASS Main Menu.

Table 5-6 provides explanations about how WASS decides whether to let you establish a secure connection. LDAP is a type of directory that stores a list of authorized users.

Table 5-6 Output Requirements to Determine System Links for User

Description
To authenticate Users, WASS queries the user information specified by the user in the User Input Requirements.
External Users must also exist in the LDAP.
If WASS login is successful, display WASS Main Menu to the User.